

FILED

UNITED STATES DISTRICT COURT

MAR 20 2024

for the
Northern District of OklahomaMark C. McCart, Clerk
U.S. DISTRICT COURT

In the Matter of the Search of
 Gold and white Apple iPhone 14, serial number
 D0QNPXQ2PK, Currently Stored at the Rogers County
 Sheriff's Office-Investigations Division Evidence Locker,
 located at 515 East Patti Page Blvd, Claremore, OK

Case No. 24-MJ-179-PJC

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed (identify the person or describe the property to be seized):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

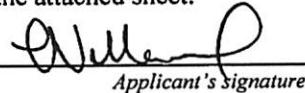
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §2252(b)	Attempted Coercion and Enticement of a Minor
18 U.S.C. §1470	Attempted Transfer of Obscene Materials to a Minor
18 U.S.C. §2252(a)(2)	Attempted Receipt of Child Pornography

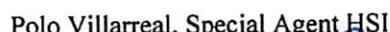
The application is based on these facts:

See Affidavit of Polo Villarreal, attached hereto.

- Continued on the attached sheet.
- Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature



Printed name and title



Judge's signature



Printed name and title

Judge F. Jayne, U.S. Magistrate Judge
 U.S. Magistrate Judge
 333 W. 4th Street
 Room 3355 U.S. Courthouse
 Tulsa, OK 74103

Subscribed and sworn to by phone.

Date: 3/20/2024

City and state: Tulsa, Oklahoma

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

In the Matter of the Search of
*Gold and white Apple iPhone 14, serial
number D0QNPXQ2PK, Currently
Stored at the Rogers County Sheriff's
Office-Investigations Division Evidence
Locker, located at 515 East Patti Page
Blvd, Claremore, OK*

Case No. _____

**Affidavit in Support of an Application
Under Rule 41 for a Warrant to Search and Seize**

I, Polo Villarreal, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant. I am a Special Agent employed by the Department of Homeland Security (DHS), Homeland Security Investigations (HSI). I have been employed as a Special Agent since April 2023 and

am currently assigned to Resident Agent-in-Charge (RAC) Tulsa. Prior to becoming a Special Agent, I was employed as a Police Officer for the Tulsa Police Department between 2018-2023. While employed by the Tulsa Police Department I was a uniformed patrol officer from 2018-2019. I was also a Detective in the Family Violence Unit from 2019-2020 and a Detective in the Cyber Crimes Unit (later renamed Sexual Predator Digital Evidence Recovery Unit) between 2020-2022. I was a member of the Oklahoma State Bureau of Investigations (OSBI) Internet Crimes Against Children (ICAC) Task Force and a Task Force Officer (TFO) for HSI 2021-2023. I have investigated over 30 cases of child exploitation cases. I graduated from the Tulsa Police Academy, the Criminal Investigator Training Program and the HSI Special Agent Training Program. I completed the 5 weeks training of Basic Computer Evidence Recovery Training hosted by the United States Secret Service at the National Computer Forensics Institute. I have also completed Cellebrite's Certified Operator and Cellebrite's Certified Physical Analyst courses in person. I have a Bachelors in Pre-Medicine Biology from University of Texas Rio Grande Valley in Edinburg, Texas.

3. As part of my duties as an HSI Special Agent, I investigate criminal violations relating to the coercion or enticement of a minor, interstate travel to engage in illicit sexual conduct, child pornography, including the production, transportation, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, 2252A, 2422, and 2423. I have received training in the areas of child pornography and child exploitation and have observed

and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in all forms of media. I have been involved in several child exploitation investigations and am familiar with the tactics used by individuals who engage in child exploitation.

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on knowledge obtained from other law enforcement officers, my review of documents related to this investigation and conversations with others who have personal knowledge of the events and circumstances described herein. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

5. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. § 2422(b)- Attempted Coercion and Enticement of a Minor, 18 U.S.C. §2252(a)(2) – Attempted Receipt of Child Pornography, and 18 U.S.C. § 1470- Transfer of Obscene Materials to Minors, will be located in the electronically stored information described in Attachment B and is recorded on the device described in Attachment A.

Identification of the Device to be Examined

6. The property to be searched is a gold and white Apple iPhone 14, with two rear cameras in a black “Otterbox” protective cover, serial number D0QNPXQ2PK, hereinafter the “Device.” The Device is currently located at Rogers County Sheriff’s

Office (RCSO) Investigative Division 515 East Patti Page Boulevard, Claremore Oklahoma, 74017 under RCSO Case Number R24007445 and Property Number 46311.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

Probable Cause

8. On March 10th, 2024, Rogers County Deputy Danielle Hamilton, through her undercover profile (UCP), on the KIK Live App, and began corresponding with an individual known as “Kyle H.” The KIK Live App is a free messaging application that uses WIFI or cellular service to communicate with others, either directly or in chat groups. In addition to its messaging capability, KIK Live allows users to join chat groups and can match users using specific criteria. Deputy Hamilton’s KIK Live undercover account identifies her as a fifteen-year-old girl and the profile picture is an aged-regressed photo of Deputy Hamilton. Kyle told UCP he was a 26-year-old male who smoked “fire” (slang term for methamphetamine). Kyle talked to UCP about smoking methamphetamine together and asked for photos of UCP. Kyle asked UCP if she would be willing to do anything for payment for the methamphetamine besides cash. When UCP asked what he was thinking, Kyle stated a “hand-job.” UCP stated a “blowjob” then Kyle said he wanted UCP to “suck it” (referring to his penis) and he asked for

a picture of UCP's butt. UCP asked Kyle to bring her a pipe to smoke the methamphetamine and Kyle agreed that he would. Kyle sent UCP a picture of what he looked like and asked UCP if she could "deep throat" and if she would be his girlfriend. Kyle asked if he could give her anal and "cum" inside her. UCP had Kyle promise that he would bring her methamphetamine in return for sex or sexual favors. Kyle told UCP that he would bring her extra meth if she would send him a picture of her butt. Kyle said he has a huge penis and that it would rip UCP's butt hole. Kyle then repeated that UCP could be his girlfriend. Kyle gave UCP his phone number to text back so that they could talk outside of the KIK Live App. Kyle sent two pictures of his fully erect penis to UCP and he told her how big he is.

9. On March 11th, 2024, at around 3:18 pm, Kyle texted UCP and told her he wanted to meet her that day because he was needing to "nut." He told UCP that if she were to "blow" him he would get her some meth in Catoosa. Kyle said she would have to give him a blow job in the truck while they were driving to pick up the meth. UCP told Kyle to meet her at the Taco Bell in Catoosa. Kyle said he would be on his way, and he would tell her when he was there.

10. Rogers County Investigators identified Kyle through the picture he sent UCP and through the phone number used to text UCP. Kyle was identified as Kyle Jackson FUGATE.

11. When FUGATE arrived at the Catoosa Taco Bell, Deputies saw him inside of a blue GMC pickup truck. FUGATE left the Taco Bell and a traffic stop was conducted as FUGATE traveled northbound on 193rd East Avenue, Catoosa,

Oklahoma.

12. FUGATE was taken into custody and read his Miranda Rights. During his interview with law enforcement, FUGATE said he attended college at Oklahoma State University in Stillwater, Oklahoma. Initially, he said he was not in the area to meet anyone and that he was in the area to get a trailer to do a skid steer job. After being confronted with some of the evidence in the case, FUGATE admitted he was at the Taco Bell to meet a girl. FUGATE admitted he communicated with the female through the Kick App. FUGATE said he thought he was meeting with a fifteen or sixteen-year-old female at Taco Bell and his intention was to have sex with her.

13. The Device is currently in the lawful possession of the Rogers County Sheriff's Office. It came into the Rogers County Sheriff's Office possession in the following way: The phone was seized search incident to arrest and placed into airplane mode. FUGATE provided his password as well as consent for investigators to go through his cellphone after he was read his Miranda Rights.

14. The Device is currently in storage at Roger's County Sheriff's Office Investigative Division, 515 East Patti Page Boulevard, Claremore, Oklahoma 74017 within the jurisdictional boundary of the Northern District of Oklahoma. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the Roger's County Sheriff's Office.

Technical Terms

15. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store

their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The

Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the

structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

16. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, access to the internet and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

Electronic Storage and Forensic Analysis

17. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

18. I know that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store electronic images. I know that in many cases, cellular telephones maintain photographs of illegal activities, including coercion and enticement of a minor, transfer of obscene materials to minors, and receipt of child pornography. These photos are sometimes stored in their cellular phones and often are transmitted or sent from one electronic media device to another. I also know that cellular phones may also contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, I know that text messages and emails are often used by two

or more persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

19. I know that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications (telephone calls and FaceTime type communications) as well as applications like "Kick Live App," "Whatsapp" and "GroupMe." Additionally, individuals utilize their cellular devices to take pictures, keep notes, as a GPS (global positioning System) device, and even to conduct illicit or illegal activity. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer conducted at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other important information to the individual. This data includes contacts used to conduct illegal activities to include coercion and enticement of a minor, transfer of obscene materials to minors, and receipt of child pornography.

20. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during and after the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, phone call histories,

contact and other information. This information may be contained on the cellular telephone.

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely

reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

18. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

19. *Methods of examination.* In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory

inspection of all information within the Device. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

Conclusion

20. Based on the information above, I submit that there is probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

21. I request to be allowed to share this affidavit and the information obtained from this search with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,

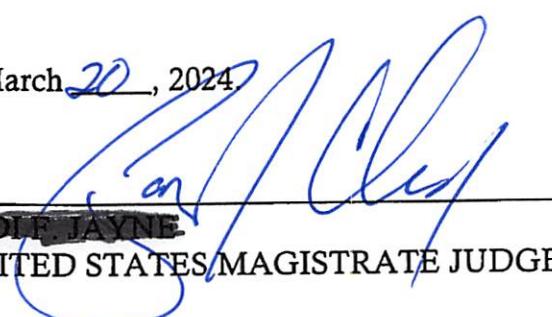


Polo Villarreal
Special Agent
Homeland Security Investigations

Subscribed and sworn to by phone on March 20, 2024



JODIE JAYNE
UNITED STATES MAGISTRATE JUDGE



Paul J. Cleary
U.S. Magistrate Judge
333 W. 4th Street
Room 3355 U.S. Courthouse
Tulsa, OK 74103

ATTACHMENT A

Property to be Searched

The property to be searched is a gold and white Apple iPhone with two rear cameras in a black "Otterbox" protective cover, serial number D0QNPXQ2PK, hereinafter the "Device." The Device is currently located at Rogers County Sheriff's Office (RCSO) Investigative Division 515 East Patti Page Boulevard, Claremore Oklahoma, 74017 under RCSO Case Number R24007445 and Property Number 46311. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

All records on the Device(s) described in Attachment A that relate to violations of 18 U.S.C. §2422(b)-Attempted Coercion and Enticement of a Minor, 18 U.S.C. §22242(a)(2)- Attempted Receipt of Child Pornography, and 18 U.S.C. § 1470, Attempted Transfer of Obscene Material to Minors, including:

1. Records relating to communication with others as to the criminal offense(s) listed above; including incoming and outgoing voice messages; text messages; emails; multimedia messages; applications that serve to allow parties to communicate; all call logs; secondary phone number accounts, including those derived from Skype, Line 2, Google Voice, and other applications that can assign roaming phone numbers; and other Internet-based communication media;
2. Records relating to documentation or memorialization of the criminal offense(s) listed above, including voice memos, photographs, videos, and other audio and video media, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos, including device information, geotagging information, and information about the creation date of the audio and video media;
3. Records relating to the planning and execution of the criminal offense(s) above, including Internet activity, firewall logs, caches, browser history, and cookies, “bookmarked” or “favorite” web pages, search terms that the user

entered into any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information;

4. Application data relating to the criminal offense(s) listed above;
5. Threatening communications related to the criminal offense(s) listed above;
6. Evidence of user attribution showing who used or owned the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, phone books, saved usernames and passwords, documents, and browsing history;
7. All records and information related to the geolocation of the Device(s) and travel in furtherance of the criminal offense(s) listed above; and
8. All records and information related to the coordination, agreement, collaboration, and concerted effort of and with others to violate the criminal statutes listed above.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and

technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.